RECORD AND BRIEFS

No. 16-402

Supreme Court, U.S.
FILED
SEP 2 - 2017
OFFICE OF THE CLERK

In The

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ Of Certiorari To The United States Court Of Appeals For The Sixth Circuit

BRIEF OF PROFESSOR ORIN S. KERR AS AMICUS CURIAE IN SUPPORT OF RESPONDENT

ORIN S. KERR
Counsel of Record
2000 H Street, NW
Washington, DC 20052
(202) 994-4775
okerr@law.gwu.edu

TABLE OF CONTENTS

Page

TABLE OF CONTENTS i

TABLE OF AUTHORITIES iii

INTEREST OF THE AMICUS CURIAE 1

SUMMARY OF ARGUMENT 1

ARGUMENT 2

I. COLLECTION OF HISTORICAL CELL-SITE DATA IS UNPROTECTED BY THE FOURTH AMENDMENT BECAUSE IT IS THE NETWORK EQUIVALENT OF OBSERVATION IN PUBLIC SPACE 3

II. THE BALANCE OF PRIVACY AND SECURITY IN HISTORICAL CELL-SITE RECORDS IS BEST RESOLVED BY LEGISLATION SUCH AS THE STORED COMMUNICATIONS ACT 7

(a) Cell Phones Can Be Used to Facilitate Crime 9

(b) Encryption Limits Government Communications Surveillance Power 11

(c) Congress and State Legislatures are Actively Engaged in Deciding the Proper Statutory Protection For Cell-Site Records 12

III. THE COURT SHOULD REJECT CARPENTER'S MOSAIC THEORY OF THE FOURTH AMENDMENT 15

TABLE OF CONTENTS – Continued

Page

IV. WHETHER REASONABLE PEOPLE EXPECT PRIVACY IN CELL-SITE RECORDS IS IRRELEVANT, AS THE THIRD PARTY DOCTRINE IS ABOUT MANIFESTING SUBJECTIVE EXPECTATIONS OF PRIVACY 20

V. THE ENACTMENT OF PRIVACY LEGISLATION DOES NOT GOVERN OR INFLUENCE THE MEANING OF THE FOURTH AMENDMENT 26

(a) Privacy Legislation Does Not Provide Evidence of Reasonable Expectations of Privacy 26

(b) 47 U.S.C. § 222 Does Not Make Cell-Site Records the User's Fourth Amendment "Papers" 29

CONCLUSION 30

TABLE OF AUTHORITIES

Page

CASES

Berger v. New York, 388 U.S. 41 (1967) 11

Dunaway v. New York, 442 U.S. 200 (1979) 15

Ex Parte Jackson, 96 U.S. 727 (1878) 7

Hester v. United States, 265 U.S. 57 (1924) 21

Hoffa v. United States, 385 U.S. 293 (1966) 21, 22, 23

Johnson v. United States, 333 U.S. 10 (1948) 10

Katz v. United States, 389 U.S. 247 (1967) ..... *passim*

Lewis v. United States, 385 U.S. 206 (1966) 21

Lopez v. United States, 373 U.S. 427 (1963) 22

Minnesota v. Carter, 525 U.S. 83 (1998) 29

New York v. Belton, 453 U.S. 454 (1981) 15, 19

On Lee v. United States, 343 U.S. 747 (1952) 22

Osborn v United States, 385 U.S. 323 (1966) 22

Riley v. California, 134 S. Ct. 2473 (2014) 8, 13, 15, 20

Rios v. United States, 364 U.S. 253 (1960) 21

Smith v. Maryland, 442 U.S. 735 (1979) 7

State v. Gray, 234 N.C. App. 197 (2014) 10

Terry v. Ohio, 392 U.S. 1 (1968) 9

United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) 29

United States v. Dionisio, 410 U.S. 1 (1973) 3

TABLE OF AUTHORITIES – Continued

Page

United States v. First National Bank, 295 F. 142 (S.D. Ala. 1924), *aff'd*, 267 U.S. 576 (1925).....7

United States v. Hill, 2013 WL 11317131 (N.D. Okla. 2013).....10

United States v. Horton, 863 F.3d 1041 (8th Cir. 2017).....8

United States v. Jacobsen, 466 U.S. 109 (1984).....25

United States v. Jeffers, 342 U.S. 48 (1951).....21

United States v. Jones, 565 U.S. 400 (2012).....15, 16

United States v. Olusola, 564 Fed.Appx. 466 (11th Cir. 2014).....10

United States v. Supreme Court of N.M., 839 F.3d 888 (10th Cir. 2016).....28

CONSTITUTIONAL PROVISIONS

Supremacy Clause.....28

U.S. Const. Amend. IV .....*passim*

STATUTES

18 U.S.C. § 2702 .....12, 24

18 U.S.C. § 2703 24

18 U.S.C. § 2703(d).....12, 20

47 U.S.C. § 222 .....26, 29

TABLE OF AUTHORITIES – Continued

Page

Cal. Penal Code
§ 1546(d) 14
§ 1546.1(b)(1) 14
§ 1546.1(d) 14

Pub. L. No. 103-414, Title II, § 207(a) (1994) 13

OTHER AUTHORITIES

Berin Szóka, *Privacy Reform Finally Moves in House: Goodlatte Promises Geolocation Privacy Bill Will Move Soon*, Tech Policy Corner, Apr. 14, 2016 14

EFF Statement on and Analysis of Digital Telephony Act, October 8, 1994 13

Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049 (2000) 30

Jake Swearingen, *No, the CIA Hasn't Compromised Signal and WhatsApp*, N.Y. Mag. Select All, Mar. 7, 2017 11

Orin S. Kerr, *A User's Guide to the Stored Communications Act, And A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208 (2004) 12

Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012) 15, 17

TABLE OF AUTHORITIES – Continued

Page

Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, Geo. L.J. (forthcoming 2018), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033 12

Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476 (2011) 7, 8, 11

Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005 (2010) 4, 5, 6

Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev. 503 (2007) 20

Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113 (2015) 21, 23, 24

Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 Mich. L. Rev. 1117 (2017) 27, 28, 29

Patricia M. Wald, *Some Observations on the Use of Legislative History in the 1981 Supreme Court Term*, 68 Iowa L. Rev. 195 (1983) 28

Susan Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)*, Berkeley Tech. L.J. (forthcoming 2018) 14

INTEREST OF THE AMICUS CURIAE

Orin S. Kerr is the Fred C. Stevenson Research Professor at the George Washington University Law School. Beginning in January 2018, he will be a Professor of Law at the University of Southern California Gould School of Law. The interest of amicus is the sound development of Fourth Amendment law.[1]

SUMMARY OF ARGUMENT

The Fourth Amendment does not apply to the collection of historical cell-site records. Collection of historical cell-site records is the network equivalent of unprotected observation in public space. Because the effect of technological change is uncertain and evolving, the Court should allow Congress and state legislatures to continue their active and dynamic debates about the proper regulation of historical cell-site records. The Court should also reject Carpenter's mosaic theory of the Fourth Amendment. The third-party doctrine should be retained, but the Court should restore it to its proper place as the subjective expectation of privacy test.

[1] All parties have consented in writing to the filing of this brief. No entity or person aside from amicus curiae made any monetary contribution supporting the preparation or submission of this brief. No counsel for any party to this proceeding authored this brief in whole or in part.

ARGUMENT

This is a challenging case. The facts involve new and developing technology. The law features vague and often-criticized tests. And the Court can't help but feel pulled by two competing and legitimate concerns. On one hand, the law must keep up as technology changes to maintain privacy protections. On the other hand, the blunt instrument of the Fourth Amendment shouldn't be forced beyond its proper role.

This brief offers a way through the difficult issues in five steps. It begins by anchoring the legal issues raised in the familiar context of the physical world. It then considers whether technological change justifies a departure from the Court's traditional rules. After that, it explains why the Court should reject the theory Carpenter advocates that would draw a distinction between longer-term and shorter-term surveillance. It next explains how the parties have misunderstood a significant part of the case, and how the case becomes much simpler when properly understood. The brief concludes by discussing the proper relationship between the interpretation of the Fourth Amendment and statutory law.

I. COLLECTION OF HISTORICAL CELL-SITE DATA IS UNPROTECTED BY THE FOURTH AMENDMENT BECAUSE IT IS THE NETWORK EQUIVALENT OF OBSERVATION IN PUBLIC SPACE.

Obtaining historical cell-site records from a cell phone provider is like obtaining testimony from an eyewitness to suspicious conduct. By contracting with a cell phone network provider to deliver their calls, customers ensure that network providers may be available to testify – whether in person or by sending records – about how the providers made that delivery for their users. Just as a person voluntarily exposes himself to observation by traveling in public to deliver a communication, so does a person voluntarily expose himself to observation by hiring an agent to deliver his communications remotely. The Fourth Amendment is not implicated by compelling testimony from an eyewitness or by observation in public. *See United States v. Dionisio*, 410 U.S. 1, 8-10 (1973); *Katz v. United States*, 389 U.S. 247, 361 (1967) (Harlan, J., concurring). The same rule should apply in the analogous context of obtaining historical cell-site records.

To appreciate this perspective, it is essential to realize that the Fourth Amendment traditionally achieves a balance between protected and unprotected conduct. On one hand, the Fourth Amendment extends constitutional protection to a person's "houses, papers, and effects" from unwarranted government interference. U.S. Const. Amend. IV. On the other hand, the

Fourth Amendment offers no protection from government surveillance in public. *See Katz*, 389 U.S. at 361.

A useful approximation of the Court's many cases is that the Fourth Amendment protects what occurs inside but doesn't protect what occurs outside. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1009-11 (2010) (hereinafter *General Approach*). This dividing line strikes an essential balance in physical-world investigations. It limits government power to protect privacy in some spaces (inside), but it allows the government to investigate without restriction in other spaces (outside). *See id.* at 1011.

When applying the Fourth Amendment to communications networks, the Court's first instinct should be to preserve this essential traditional balance. To ensure that the balance of the Fourth Amendment is maintained in our increasingly networked technological world, the Court should translate the law's treatment of physical world space across the shift to a networked environment. This is necessary to maintain the traditional degree of privacy protection the Fourth Amendment offers as technology changes.

Translation produces a simple rule: Although the Fourth Amendment protects the contents of communications sent over a network, it does not protect non-content addressing information used to deliver those contents. *See General Approach* at 1017-22. Judge Kethledge properly recognized in his opinion below that the Court's precedents have adopted the content/

non-content distinction in its caselaw on postal letters and telephone calls. Pet. App. 9a-13a. But the content/non-content line is essential for a deeper reason beyond precedent. It recreates the inside/outside distinction from the physical world, protecting the network equivalent of inside surveillance (contents) and leaving unprotected the network equivalent of outside surveillance (non-content records). *See General Approach* at 1017-22.

To see this, imagine a world without communications networks. If Alice wants to communicate with Bob, Alice has to leave her home and travel to Bob's house. If the police suspect that Alice and Bob are conspirators planning a crime, and they assign an officer to watch Alice's whereabouts, the police can collect only some information without triggering the Fourth Amendment. The police cannot learn the contents of what Alice and Bob said inside Bob's home without a warrant. On the other hand, the police can observe Alice and see what she did in public – when she left home, where she traveled, when she arrived at Bob's house, and where they both live – without triggering the Fourth Amendment.

Next imagine that Alice calls Bob on her cell phone instead of meeting him in person. Alice no longer has to travel to meet Bob. The cell phone network delivers the call from Alice to Bob, making a remote transfer that eliminates the need for a public trip. But, critically, the same information exists. What was previously the contents of the conversation in Bob's house is now the contents of the phone call between Alice and

Bob. And what was previously Alice's publicly observable trip from her house to Bob's house is now a record that the phone provider generated and may keep about when the call was made, to and from what numbers, and what cell towers were used to deliver it.

To maintain the balance of the Fourth Amendment, courts should treat the same information in the same way in both the physical and network contexts. The contents of phone calls should be protected, as they are the telephone equivalent of protected inside space. This means, in the Internet context, that the contents of e-mails, text messages, and files that users place in cloud storage should receive full Fourth Amendment protection. *See General Approach* at 1029. On the other hand, non-content records generated by network providers – the business records they generate about how they delivered the communications – should not be protected because they are the network equivalent of the publicly observable trip that is outside such protection in the physical world. *See id.* at 1017-22.

It is true, as Carpenter argues, that cell phones are "indispensable for full participation in family, social, professional, civic, and political life." Petr. Br. at 40. But that provides no more reason to protect cell-site records than does the normal human need to venture outside provide reason to protect observation in public. The Fourth Amendment extends protection to some aspects of life but leaves other parts unprotected both in the physical world and in the network environment.

This approach should lead the Court to reaffirm the traditional rule, over a century old, that collection of non-content addressing information for a network communication does not implicate the customer's Fourth Amendment rights. *See Ex Parte Jackson*, 96 U.S. 727, 733 (1878) (postal letters); *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (telephone calls). *See also United States v. First National Bank*, 295 F. 142, 143 (S.D. Ala. 1924) (rejecting a challenge to government access to a couple's entire bank records, stating that "[t]his is not a question of a search and seizure of a party's books and papers, but of whether a witness who has information as to a party's dealings may be required to testify to those facts"), *aff'd*, 267 U.S. 576 (1925) (per curiam).

II. THE BALANCE OF PRIVACY AND SECURITY IN HISTORICAL CELL-SITE RECORDS IS BEST RESOLVED BY LEGISLATION SUCH AS THE STORED COMMUNICATIONS ACT.

But wait, Carpenter says: Cell phone technology has expanded government power to invade privacy. In petitioner's view, changing technology justifies adding new protection for cell-site records to restore the prior level of government power. Petr. Br. at 14-21. I have called this argument "equilibrium-adjustment." I agree with Carpenter that, in a proper case, equilibrium-adjustment is an appropriate way to update Fourth Amendment rules in light of technological change. *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476,

525-42 (2011) (hereinafter *Equilibrium-Adjustment*). Technological change that dramatically expands government power under old legal rules can justify imposing greater privacy protection. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473, 2494 (2014) (requiring a warrant to search a cell phone incident to arrest because of "all they contain and all they may reveal"); *Equilibrium-Adjustment* at 525-42.

This is not such a case, however. First, Carpenter exaggerates the threat to privacy posed by historical cell-site records. Such records ordinarily cover too broad an area to be particularly revealing on their own. Resp. Br. at 24-28. Notably, Carpenter does not say what personal or sensitive fact was learned about him, other than his location generally near a string of robberies, when the government collected his records.[2] Carpenter's brief instead focuses on the privacy threat raised by different location technologies such as GPS

---

[2] The Technology Experts claim that the records show Carpenter "attended a particular church in Detroit nearly every Sunday." Brief of Amici Curiae Technology Experts at 29 n.49. That is wrong. According to an amicus brief filed in the Sixth Circuit, Carpenter told amicus counsel that he attended a particular church. *See* Brief of Amicus Curiae Am. Civil Liberties Union et al. at 11, 819 F.3d 880 (2016) (Nos. 14-1572 & 14-1805), available at https://www.aclu.org/legal-document/united-states-v-carpenter-amicus-brief. Analysis of the cell-site records then showed that on "a number of Sundays," Carpenter's phone was used in sectors that included that church. *Id.* This provides no basis to conclude that the records, considered alone, would have revealed church attendance. The reason to think Carpenter attended a particular church is that he said so.

tracking. *See* Petr. Br. at 19-29, 42-47. Those technologies typically require access to information stored inside a person's physical device, however, and therefore their use may be searches under traditional Fourth Amendment principles. *See, e.g.*, *United States v. Horton*, 863 F.3d 1041, 1047 (8th Cir. 2017).

More fundamentally, technology's impact on government communications surveillance power is decidedly mixed. Although cell phone technology expands government power in some ways, it shrinks government power in other ways that Carpenter ignores. A close look at two dynamics – how cell phones can facilitate crime and the role of encryption – suggests that the overall impact of technology on government surveillance power is uncertain and still evolving.

(a) Cell Phones Can Be Used to Facilitate Crime.

Cell phone technology can limit government power by giving wrongdoers a powerful new way to avoid detection in the commission of crime. Consider the impact of cell phones on a group robbery such as the one in this case. Before the cell phone age, conspirators planning to rob a store had to "case the joint" in the open and meet in person to coordinate their plans. Their suspicious behavior risked drawing the attention of officers nearby. *See Terry v. Ohio*, 392 U.S. 1 (1968) (permitting an officer to "stop and frisk" conspirators acting suspiciously in front of a store in the course of planning a robbery).

Cell phones make such crimes easier to commit and harder to detect. These days, robbery conspirators can coordinate their crimes silently and instantly over any distance by cell phone text message. One conspirator can watch the store and text his observations to the others. *See, e.g.*, *State v. Gray*, 234 N.C. App. 197, 206 (2014). A second conspirator can serve as a lookout and text the group if danger appears. *See United States v. Olusola*, 564 Fed.Appx. 466, 468 (11th Cir. 2014). After the robbery, the leader can text the rest with instructions about where to meet to divvy up the loot. *See, e.g.*, *United States v. Hill*, 2013 WL 11317131, *2 (N.D. Okla. 2013). The cell phone replaces awkward and suspicious in-person meetings with concealed, silent, and instant coordination. An officer walking the beat will be none the wiser. The conspirators will look like everyone else: Just people checking their phones.

The ways that cell phones can facilitate crime and avoid detection counsels against creating new Fourth Amendment protections for cell phone records. Obviously, most people don't use their phones to commit crimes. But most people don't have their records collected by court order under the Stored Communications Act, either. The key point is that the effect of cell phone technology on the "often competitive enterprise of ferreting out crime," *Johnson v. United States*, 333 U.S. 10, 14 (1948), operates as a two-way street. The ability of cell phone companies to deliver communications quickly and silently over any distance cuts both ways. It can lead to records about the delivery that helps the police, and it can aid in the commission of

crime that helps wrongdoers. Both should be considered. *See Equilibrium-Adjustment* at 512-17.

(b) Encryption Limits Government Communications Surveillance Power.

The rise of encryption also complicates the dynamic Carpenter describes. In the past, the government ordinarily had the technical capacity to intercept the contents of phone calls and communications. *See Berger v. New York*, 388 U.S. 41, 46 (1967). In the last decade, however, software providers have provided powerful and free technologies that enable anyone to shield the contents of their communications from lawful government access by encrypting the contents of their network communications during transmission. For example, today over one billion people worldwide use "WhatsApp," a program first introduced in 2009 that encrypts messages end-to-end. *See* Join WhatsApp.[3] As far as the public knows, not even the Central Intelligence Agency can break WhatsApp's encryption. *See* Jake Swearingen, *No, the CIA Hasn't Compromised Signal and WhatsApp*, N.Y. Mag. Select All, Mar. 7, 2017.[4] Doing so is presumably beyond the capacity of federal, state, or local law enforcement.

Encryption shows how the impact of technology on government communications surveillance power can work both ways. Encryption brings many wonderful

---

[3] https://www.whatsapp.com/join/

[4] http://nymag.com/selectall/2017/03/no-the-cia-hasnt-cracked-encrypted-chat-app-signal.html

benefits, but it can leave investigators unable to read a target's encrypted communications even with a search warrant. It is too early to tell how far encryption will interfere with government investigative powers.[5] But because users generally can't encrypt non-content records such as historical cell-site records, the collection of such records may take on a more important role in future surveillance practices. The Court should be reluctant to introduce new constitutional protections for non-content records when the existing constitutional framework for access to contents may be impeded by new encryption technology.

(c) Congress and State Legislatures are Actively Engaged in Deciding the Proper Statutory Protection For Cell-Site Records.

Because the effect of technology on communications surveillance is a mixed bag, the Court should continue to allow legislatures to debate and decide how much protection cell-site records should receive. The federal Stored Communications Act sets a floor for all investigators. *See* 18 U.S.C. § 2702, § 2703(d). *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, And A Legislator's Guide to*

---

[5] Law enforcement can try several ways to work around encryption to access contents. *See generally* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, Geo. L.J. (forthcoming 2018), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033. These methods may or may not work, however, and some require considerable resources beyond the reach of many criminal investigations. *See id.* at 33-35.

Amending It, 72 Geo. Wash. L. Rev. 1208, 1209-25 (2004) (summarizing the privacy protections of the Stored Communications Act). The states are free to impose greater restrictions on state and local officers. The Court should not short-circuit this active and dynamic legislative process by imposing a one-size-fits-all constitutional rule. *See Riley*, 134 S. Ct. at 2497-98 (Alito, J., concurring in the judgment).

Legislators certainly recognize the need for some kind of statutory privacy protection limiting government access to cell-site records. Everybody gets that. The real debate is over what standards and remedies should govern. In 1994, Congress amended the Stored Communications Act to impose a new "specific and articulable facts" standard for access to non-content historical network account records that include cell-site records. *See* Pub. L. No. 103-414, Title II, § 207(a) (1994). At the time, amicus curiae Electronic Frontier Foundation celebrated the new privacy law as a "critical" measure that achieved "a significantly greater level of protection" than traditional network privacy laws. *See* EFF Statement on and Analysis of Digital Telephony Act, October 8, 1994.[6]

Since 1994, Congress has frequently debated whether to further raise the statutory standard for access to cell-site records. By my count, the House Judiciary Committee and its subcommittees have held

---

[6] https://w2.eff.org/Privacy/Surveillance/CALEA/digtel94_passage_statement.eff

hearings partly or largely about this question five different times – in 2000, 2010 (twice), 2012, and 2013.[7] Committee Chair Robert Goodlatte promised last year that more legislative attention was coming. *See* Berin Szóka, *Privacy Reform Finally Moves in House: Goodlatte Promises Geolocation Privacy Bill Will Move Soon*,[8] Tech Policy Corner, Apr. 14, 2016.

State legislatures have also been active. California recently enacted the most far-reaching statutory privacy protection for network and electronic communications ever seen in the United States. *See generally* Susan Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)*, Berkeley Tech. L.J. (forthcoming 2018).[9] Starting in 2016, the law not only requires a warrant for California law enforcement access to non-content records, including historical cell-site data, but it also imposes special particularity and nondisclosure rules for those warrants. *See* Cal. Penal Code § 1546(d), § 1546.1(b)(1), § 1546.1(d).

---

[7] The published reports of these hearings are available here:

bit.ly/HouseReport2000

bit.ly/HouseReport20101

bit.ly/HouseReport20102

bit.ly/HouseReport2012

bit.ly/HouseReport2013

[8] https://techpolicycorner.org/email-privacy-reform-finally-moves-in-house-df8f09962de6

[9] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2939412

III. THE COURT SHOULD REJECT CARPENTER'S MOSAIC THEORY OF THE FOURTH AMENDMENT.

Carpenter chiefly argues that the Court should follow the concurring opinions in *United States v. Jones*, 565 U.S. 400 (2012), which suggested that certain kinds of long term surveillance can become a Fourth Amendment search. Petr. Br. at 14-32. The *Jones* concurring opinions reflect the so-called "mosaic theory," by which government evidence-collection is not a search in isolation but becomes a search when aggregated and analyzed over some period of time to create a mosaic picture of a person's activities. *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012) (hereinafter *Mosaic Theory*).

A majority opinion of the Court has never adopted the mosaic theory. And it should not start now. The mosaic approach is well-intentioned but deeply misguided. It is a dramatic departure from traditional approaches, and it would drag state and federal courts into impossible line-drawing exercises that would cause endless confusion. Adopting the mosaic theory "would keep defendants and judges guessing for years to come," *Riley*, 134 S. Ct. at 2493, instead of providing the bright-line rules that are "essential to guide police officers." *New York v. Belton*, 453 U.S. 454, 458 (1981) (quoting *Dunaway v. New York*, 442 U.S. 200, 213-14 (1979)).

Before discussing the problems with the mosaic theory, it's important to realize that the *Jones* concurrences themselves suggest it may not apply to collection of historical cell-site records. Both concurrences in *Jones* were premised at least in part on the absence of legislation limiting the executive branch. *See Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (suggesting that the appropriateness of permitting executive discretion should be considered "in the absence of any oversight from a coordinate branch"); *id.* at 430 (Alito, J., concurring in the judgment) (justifying the approach because legislatures "have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes"). As discussed above, the collection of historical cell-site records is the subject of extensive statutory regulation at both the federal and state levels. The *Jones* concurrences are distinguishable on that basis alone.

If the Court must address the general viability of the mosaic theory, the approach should be rejected. Under the "longer term" aggregation approach advocated by Carpenter, the basic operation of Fourth Amendment doctrine would be thrown into doubt. The Court would need to answer an extensive list of novel and difficult questions to allow lower courts to implement the short-term/long-term distinction. In effect, the Court would need to create a parallel set of new Fourth Amendment rules. This would be a remarkable challenge. The Court should not adopt the mosaic approach without recognizing the complexities ahead.

I elaborate on the difficult questions in my *Mosaic Theory* article, *see id.* at 328-43, but here is an overview of the main questions. First, which surveillance methods are covered by a mosaic approach? If the mosaic theory applies to collection of historical cell-site records, does it also apply to collecting credit card records? Bank records? Use of automatic license plate readers? Use of public cameras installed by the government? Collection of camera footage from cameras installed by private actors? Monitoring of phone numbers dialed or Internet Protocol addresses used? Visual surveillance? Does the mosaic approach apply only to collecting location information, or does it apply to collecting any information – and if it is limited to location records, what about records (such as credit card statements) that permit plausible guesses about a person's location? Each technique, and many more, would need to be classified as included or excluded.

For each technique covered by the mosaic theory, a host of questions would arise. The most obvious – how long counts as "longer term" – is just the tip of the iceberg. Other questions include: Is the time period the same for different surveillance methods covered by the mosaic approach? What if several people used the device and no mosaic for any one individual can be constructed? And imagine the government uses two surveillance methods at the same time, such as GPS and cell-site tracking together, to monitor a suspect. Does that cut the window of allowed monitoring in half?

It gets even more complicated. Imagine the Court tries to draw a bright-line rule. Let's imagine, for the sake of argument, that 21 days of surveillance always triggers a mosaic search. Does switching surveillance methods restart the clock? For example, can the police do 20 days of GPS tracking, then 20 days of cell-site monitoring, and then 20 days of Internet Protocol address monitoring? Or does each day of any surveillance method count towards the 21-day total?

And is there a statute of limitations that resets the clock? Imagine investigators collect 20 days of cell-site records to avoid a search. Can they wait six months – or a year or two – and then get another 20 days' worth? And what if they get records only covering four hours per day, say, from 1pm to 5pm every day. Can they still only get records for 21 individual days before triggering a search, or can they now get records for up to 126 days because they are only collecting records for part of each day? And consider how the test works if there are multiple investigations of the same suspect, such as a federal investigation and a local investigation operating concurrently. Does the 21-day rule apply to all investigators collectively, or does separation among investigations mean different 21-day clocks?

Next consider how to determine the reasonableness of a mosaic search and what remedies apply to violations. Is a warrant required? If so, how can a mosaic warrant satisfy the particularity requirement when it is inherently about aggregating surveillance

from many places over time? If no warrant is required, how much cause is required? Do all mosaic searches require the same amount of cause, or do different mosaic techniques for time periods trigger different levels? What is the test for standing to challenge a mosaic search? Does the exclusionary rule apply, and if so does it apply to the entire surveillance that occurred or only that which crossed the line into being a search?

Carpenter offers no answers to these questions. "When the time comes to provide precise guidance to law enforcement agents and lower courts," Carpenter writes, "this Court will have ample authority to do so." Petr. Br. at 30. Carpenter won't even touch the simplest question of how long is "longer term." In some future case, Carpenter says, the Court can "set bright-line durational limits." *Id.* at 31. Just adopt the theory now, in other words. You can confront the maddening implications of it later.

The Court should decline this invitation. Fourth Amendment law requires certainty, *see Belton*, 453 U.S. at 458, in part because the blunt instrument of the exclusionary rule may apply. Because the government can lose its case if officers break the law, courts must provide clear rules that enable investigators to steer clear of violations. It is hard to see how courts can supply those clear answers under a mosaic theory. The many questions it raises "would keep defendants and

judges" – and for that matter, law professors – "guessing for years to come." *Riley*, 134 S. Ct. at 2493.[10]

IV. WHETHER REASONABLE PEOPLE EXPECT PRIVACY IN CELL-SITE RECORDS IS IRRELEVANT, AS THE THIRD PARTY DOCTRINE IS ABOUT MANIFESTING SUBJECTIVE EXPECTATIONS OF PRIVACY.

The parties frame this case as being largely about the reasonable expectation of privacy test. That test has been the subject of extraordinary confusion. Both courts and commentators have been unsure of what makes an expectation of privacy "reasonable." The uncertainty is understandable. The Court has mixed and matched among four different frameworks that offer different answers to what makes an expectation of privacy reasonable. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev. 503 (2007). I have called these four frameworks the probabilistic, private facts, positive law, and policy models. *See id.* at 507-24. A close read of Carpenter's brief reveals rotating use of each of the four models. *See* Petr. Br. at 14-15 (probabilistic model); *id.* at 15-21 (policy

---

[10] For this reason, if the Court concludes that the Fourth Amendment governs government collection of historical cell-site records, the same Fourth Amendment restriction should apply to both short-term and long-term records collection. In that event, the Court should also conclude that the intermediate standard of 18 U.S.C. § 2703(d) satisfies the Fourth Amendment. *See* Resp. Br. at 50-55.

model); *id.* at 21-23 (positive law model); *id.* at 24-29 (private facts model).

Fortunately, the Court can and should sidestep the morass of the reasonable expectation of privacy test in this case. Properly understood, this case is not about the reasonable expectation of privacy test at all. Instead, like other cases concerning the third-party doctrine, it is actually about the subjective expectation of privacy test. *See* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113, 115, 127-29 (2015) (hereinafter *Subjective Expectations*). From this perspective, Carpenter's position attempts to eliminate the original intended role of the subjective prong of the two-part *Katz* test that the Court has adopted. *See id.* at 115. The Court should reject Carpenter's invitation to set the Fourth Amendment on that new and uncharted path.

Appreciating this point requires a close read of Justice Harlan's famous concurring opinion in *Katz*. At the time of *Katz*, there were two distinct sets of Fourth Amendment precedents on what is a search. One set identified the spaces that could be the subject of Fourth Amendment protection. *See, e.g.*, *Rios v. United States*, 364 U.S. 253 (1960) (taxi cab); *United States v. Jeffers*, 342 U.S. 48, 51-52 (1951) (hotel room). *But see Hester v. United States*, 265 U.S. 57, 59 (1924) (open fields). The second set considered when a person waived protection in an otherwise-protected space by voluntarily revealing information to others such as undercover agents. *See, e.g.*, *Hoffa v. United States*, 385 U.S. 293, 302 (1966); *Lewis v. United States*, 385 U.S.

206, 210-11 (1966); *Osborn v. United States*, 385 U.S. 323, 325-27 (1966); *Lopez v. United States*, 373 U.S. 427, 438-39 (1963); *On Lee v. United States*, 343 U.S. 747, 749 (1952).

Justice Harlan's two-part *Katz* test simply summarized that case law. The "twofold requirement" was Justice Harlan's "understanding of the rule that has emerged from prior decisions" that explained how the Fourth Amendment protected a "place." *Katz*, 389 U.S. at 360 (Harlan, J., concurring). One requirement was that the government intrusion of a protected area be "a place" about which "society is prepared to recognize" an "expectation of privacy" as "reasonable." *Id.* This answered what spaces could be constitutionally protected. Conversation in homes and enclosed phone booths could be protected but "conversations in the open would not be protected." *Id.* at 360-61.

Another requirement was that a person must "have exhibited an actual (subjective) expectation of privacy." *Id.* at 361. Under this requirement, "objects, activities, or statements that he exposes to the plain view of outsiders" from inside a constitutionally protected space "are not protected because no intention to keep them to himself has been exhibited." *Id.* This accurately summarized the many cases holding that a person had no Fourth Amendment protection against the use of undercover agents even inside the home. *See, e.g.*, *Hoffa*, 385 U.S. at 302-03. The key was that an expectation of privacy had to be "exhibited," that is, demonstrated by an act. A person had to shield his speech from others to have protection; one who shared

information with others necessarily accepted the risk they would reveal it. *See id.*

All of this matters because *Carpenter* is about the second inquiry rather than the first. No one is characterizing the "place" where the cell-site records were obtained or stored. It is irrelevant whether "society is prepared to recognize" an expectation of privacy in that place as reasonable. This case instead is about cell-phone users' failure to exhibit a subjective expectation of privacy against a phone company's network connecting with the phone to route the user's communications. Using a phone that seeks a connection with local networks does not exhibit an expectation of privacy in the fact of that connection. Properly understood, the reasonable expectation of privacy test has no bearing on the issues raised in this case.

As I detailed in a recent article, some precedents of this Court have confused this point. *See Subjective Expectations* at 124-26. The "subjective" prong of the *Katz* test was wrongly assumed to be truly subjective. This confusion led the Court to move the disclosure principle over to the objective part of the test under the label of the so-called third-party doctrine. *Id.* The result is a doctrinal oddity. The two-part *Katz* test has been reduced to one part, and the third-party doctrine that was originally the subjective part of *Katz* is now a special application of the objective part. *Id.* at 127-33. No wonder so many scholars criticize the third-party doctrine: It comes off as a strange application of the reasonable expectation of privacy test. But that's because it's not an application of that test at all. The

Court should retain the third-party doctrine but characterize it properly as the subjective test, recognizing that it is distinct from the reasonable expectation of privacy test.[11]

This background explains the inability of Carpenter and his amici to identify a clear rule to govern this case. Carpenter seeks to do something truly new. He wants to introduce a right to stop others (here, cell phone companies) from disclosing to the government information he has shared with them. Carpenter can't identify a clear rule because no Fourth Amendment principle explains who can be stopped to talk about what they know and what facts they can't disclose. Any doctrinal line would be made out of thin air.

That poses no problem for legislatures. Legislatures can enact a nondisclosure rule that prohibits specific entities from disclosing specific kinds of information except pursuant to specific kinds of legal process. Congress has done exactly that in the Stored Communications Act. *See* 18 U.S.C. § 2702, § 2703. But it's hard to introduce a Fourth Amendment nondisclosure rule to determine what is a search. No constitutional text, history, or caselaw offers guidance on what

---

[11] In my *Subjective Expectations* article, I recommended eliminating the subjective prong while retaining the third-party doctrine. *See id.* at 133-34. I now think the more sensible approach is to restore the original understanding of *Katz* with the third-party doctrine properly labeled the subjective prong and distinguished from the objective prong.

such a private-party nondisclosure rule would look like.

The Empirical Scholars look for answers in public opinion polls and surveys. *See* Amicus Brief of Empirical Fourth Amendment Scholars at 2-10. They envision the *Katz* test as protection against the unexpected: Surprising disclosures to the government should require a warrant because they violate the expectations of ordinary people. *See id.* at 10-16. That has never been the law. "The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, *however well justified*, that certain facts will not come to the attention of the authorities." *United States v. Jacobsen*, 466 U.S. 109, 122 (1984) (emphasis added).

Nor should it become the law. The Constitution already includes an institution, Congress, that is designed to reflect public opinion about disclosures of information. It's also hard to see why the Fourth Amendment should protect against unexpected government action. And what disclosures are surprising to people is likely based on what they read on the Internet, which is not exactly a reliable basis for constitutional decisionmaking. Finally, it would be difficult for courts to implement a survey-based approach to what disclosures of information should be a search. Public opinion changes, and judges are not empiricists who are trained to compare and critique new scholarly research. Empirical studies can be useful in some contexts within Fourth Amendment law. But they cannot

Court should retain the third-party doctrine but characterize it properly as the subjective test, recognizing that it is distinct from the reasonable expectation of privacy test.[11]

This background explains the inability of Carpenter and his amici to identify a clear rule to govern this case. Carpenter seeks to do something truly new. He wants to introduce a right to stop others (here, cell phone companies) from disclosing to the government information he has shared with them. Carpenter can't identify a clear rule because no Fourth Amendment principle explains who can be stopped to talk about what they know and what facts they can't disclose. Any doctrinal line would be made out of thin air.

That poses no problem for legislatures. Legislatures can enact a nondisclosure rule that prohibits specific entities from disclosing specific kinds of information except pursuant to specific kinds of legal process. Congress has done exactly that in the Stored Communications Act. *See* 18 U.S.C. § 2702, § 2703. But it's hard to introduce a Fourth Amendment nondisclosure rule to determine what is a search. No constitutional text, history, or caselaw offers guidance on what

---

[11] In my *Subjective Expectations* article, I recommended eliminating the subjective prong while retaining the third-party doctrine. *See id.* at 133-34. I now think the more sensible approach is to restore the original understanding of *Katz* with the third-party doctrine properly labeled the subjective prong and distinguished from the objective prong.

such a private-party nondisclosure rule would look like.

The Empirical Scholars look for answers in public opinion polls and surveys. *See* Amicus Brief of Empirical Fourth Amendment Scholars at 2-10. They envision the *Katz* test as protection against the unexpected: Surprising disclosures to the government should require a warrant because they violate the expectations of ordinary people. *See id.* at 10-16. That has never been the law. "The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, *however well justified*, that certain facts will not come to the attention of the authorities." *United States v. Jacobsen*, 466 U.S. 109, 122 (1984) (emphasis added).

Nor should it become the law. The Constitution already includes an institution, Congress, that is designed to reflect public opinion about disclosures of information. It's also hard to see why the Fourth Amendment should protect against unexpected government action. And what disclosures are surprising to people is likely based on what they read on the Internet, which is not exactly a reliable basis for constitutional decisionmaking. Finally, it would be difficult for courts to implement a survey-based approach to what disclosures of information should be a search. Public opinion changes, and judges are not empiricists who are trained to compare and critique new scholarly research. Empirical studies can be useful in some contexts within Fourth Amendment law. But they cannot

provide the nondisclosure line-drawing that Carpenter needs.

V. THE ENACTMENT OF PRIVACY LEGISLATION DOES NOT GOVERN OR INFLUENCE THE MEANING OF THE FOURTH AMENDMENT.

Carpenter also argues that the enactment of privacy legislation should lead the Court to hold that he has Fourth Amendment rights in his cell-site records. He makes this argument in two ways. First, he argues that the existence of statutory privacy protections for cell-site records reflect a societal expectation of privacy in those records. Petr. Br. at 21-23. Second, he argues that designations found in 47 U.S.C. § 222 create a proprietary interest that makes cell-site records the user's constitutional "papers" or "effects." Petr. Br. at 32-35.

Both arguments should be rejected.

(a) Privacy Legislation Does Not Provide Evidence of Reasonable Expectations of Privacy.

The enactment of privacy legislation cannot bolster Carpenter's case for constitutional protection for two reasons. The first reason is implicit in the discussion above: Because this case *is* properly understood as being about a failure to manifest a subjective expectation of privacy rather than reasonable expectations of privacy, whatever reasonable expectations may exist are not relevant. *See* Part IV, *supra*. The second reason

is broader and more fundamental. Even if you assume that this is a case about reasonable expectations of privacy, privacy legislation cannot provide a helpful guide to assessing those expectations.

Here are the basic problems, drawing from a recent article that explores the issue in greater depth. *See* Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 Mich. L. Rev. 1117 (2017) (hereinafter *Effect of Legislation*). First, privacy legislation does not signal Fourth Amendment values because it answers a very different set of questions. Any legal regime regulating law enforcement access must address three questions: What information is covered, how much protection is given to what is protected, and what remedies apply to violations. Because legislative privacy laws typically answer all three questions differently from Fourth Amendment law, one can't isolate any specific answer and imagine it sheds light on the constitutional framework when the two other answers are different. *Id.* at 1140-44.

The Stored Communications Act offers an example. Although the federal statute protects cell-site records from disclosure, that protection offers no guidance on whether the Fourth Amendment should do so. The statute imposes no limit on the scope of records obtained; it uses a "specific and articulable facts" disclosure standard; and it rejects a statutory exclusionary rule. Pet. App. 17a-18a. It's not clear how the coverage of the statute can inform a judgment about whether the Fourth Amendment should apply given that the

Fourth Amendment typically has a different scope, a different standard, and different remedies. *See Effect of Legislation* at 1140-44.

The same is true with state laws that adopt a warrant requirement for access to historical cell-site records. Even assuming the exclusionary rule applies to violations of those statutes, the states only have the constitutional authority to regulate state and local governments. Under the Supremacy Clause, state laws cannot regulate federal investigations. *See, e.g.*, *United States v. Supreme Court of N.M.*, 839 F.3d 888 (10th Cir. 2016). This makes it difficult to determine the lesson of a state law warrant requirement. Does it signal a wish to impose strong protection against disclosure of cell-site records, or does it signal only a wish to regulate collection by state and local officers? *See Effect of Legislation* at 1144-47.

Further, if the adoption of warrant-based protections by a minority of states signals something about the Fourth Amendment, what should we make of the fact that a majority of states have not enacted such protections? Does that mean most states see no privacy implications in the disclosure of cell-site data? That most states are fine with the federal standard? That most states just haven't yet reached the question? Looking at state laws for insights about privacy expectations requires drawing lessons from very mixed signals. Like mining legislative history for helpful comments, it is akin to "looking over a crowd and picking out your friends." Patricia M. Wald, *Some Observations on the Use of Legislative History in the 1981 Supreme*

Court Term, 68 Iowa L. Rev. 195, 214 (1983) (quoting Judge Harold Leventhal). The better approach is to interpret the Fourth Amendment independently of statutory privacy protections. *See Effect of Legislation* at 1157-64.

(b) 47 U.S.C. § 222 Does Not Make Cell-Site Records the User's Fourth Amendment "Papers".

Carpenter's argument that 47 U.S.C. § 222 makes cell-site records the customer's Fourth Amendment "papers" should also be rejected. To be sure, the Fourth Amendment concept of "papers" includes papers in electronic form. *See Katz*, 389 U.S. at 362 (Harlan, J., concurring); *United States v. Ackerman*, 831 F.3d 1292, 1304 (10th Cir. 2016) (Gorsuch, J.). At the same time, the Fourth Amendment only provides a right to persons in "their" papers, not in the papers of someone else. U.S. Const. Amend. IV; *Minnesota v. Carter*, 525 U.S. 83, 92-97 (1998) (Scalia, J., concurring).

The cell-site records collected in this case were the "papers" of the phone companies, not Carpenter. Cell-site records are information that a company creates, and a company then decides to store on its computers, about how the company's network was used. Users have no legal right to access their cell-site records. The records belong to the companies not their users. *Cf. id.* (Scalia, J., concurring).

Carpenter's argument to the contrary is based on 47 U.S.C. § 222, which imposes certain limitations on

the disclosure of customer-related records. The problem is that rules regulating disclosure do not create a property right in the regulated facts that belong to the subject of the disclosure. Confidentiality is not property. The fact that information concerns someone does not make that information his stuff. If the law limits when Alice can tell the world about what she saw Bob do, Alice's recollection does not become Bob's "papers" or "effects." Alice's recollections belong to Alice, not Bob. *Cf.* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049, 1063-81 (2000).

CONCLUSION

The judgment of the court of appeals should be affirmed.

Respectfully submitted,

ORIN S. KERR
Counsel of Record
2000 H Street, NW
Washington, DC 20052
(202) 994-4775
okerr@law.gwu.edu

October 2, 2017